Kiteworks

SOLUTION BRIEF

FOR CISOS, COMPLIANCE OFFICERS, AND DEFENSE CONTRACTORS

How DIB Suppliers Should Stop a Phished Login from Undermining CMMC Certification

A Compromised Mailbox Exposed Purchase Orders, Engineering Data, and Export-Controlled Files. See How Kiteworks Closes the Gap Between a Login and Everything Behind It.

CMMC 2.0 | ITAR | DFARS 7012 | Email Protection Gateway

The Challenge

In August 2026, a phished credential gave an intruder standing access to defense connector maker IEH Corporation's Microsoft 365 mailbox for an unknown length of time. IEH, whose parts fly inside the PATRIOT air-defense system, AMRAAM, THAAD, and the MARK-48 torpedo, disclosed that the compromised account exposed purchase orders, engineering documentation, and potentially export-controlled technical data — and that it could not determine how long the access had gone unnoticed (The Register, August 2026).

That is not a failure unique to one IT team. Credential phishing routinely defeats identity controls, and once an attacker is inside a mailbox, native email platforms store years of correspondence as plaintext with no independent layer of protection or audit trail built to answer what an account touched and for how long. For defense contractors, the stakes compound: CMMC 2.0's third-party assessment requirement was suspended by the Department of Defense in July 2026, leaving self-attestation as the only safeguard on most of the defense industrial base for the foreseeable future.

The Solution

Kiteworks Email Protection Gateway (EPG) moves policy enforcement into the mail stream itself, so a compromised credential does not automatically become a compromised archive. Every inbound and outbound message is encrypted, quarantined, or routed under policy the moment it is sent or received, based on the sensitivity of the data involved, not on whether an employee remembers to protect it. Sensitive and export-controlled content carries its own digital rights controls — view-only access, expiration, no forwarding — so it stays governed even after delivery, independent of who is logged into the account.

A unified, immutable audit log captures every policy decision on every message, giving security and compliance teams the evidence an assessor, an auditor, or a regulator will eventually ask for. That evidence closes exactly the gap self-attestation leaves open: instead of a once-a-year score, contractors get a continuous, defensible record of what left the building, who touched it, and when — the record IEH's own team could not produce when asked how long its mailbox had been exposed.

The Exposure Is Not Theoretical

Sources: 2026 Verizon Data Breach Investigations Report; CrowdStrike 2026 Threat Hunting Report; U.S. GAO-26-108606 (July 2026).

62%
Of Breaches Involve the Human Element

15x
Rise in Device-Code Phishing, H1 2026

70%
Of Federal Cyber Rules Duplicate Another

How Kiteworks Email Protection Gateway Closes the Gap

Automated Policy Enforcement

Every message is encrypted, quarantined, or routed automatically by data sensitivity, not user judgment.

Digital Rights Management

View-only access, expiration, and forwarding controls travel with sensitive attachments, even after they are delivered.

Sensitivity Label Integration

Reads Microsoft Purview labels and applies the correct handling to CUI and export-controlled data automatically.

How Kiteworks Email Protection Gateway Closes the Gap

Inbound Threat Scanning

DLP, antivirus, and advanced threat protection screen every message before it reaches an employee's inbox.

Unified, Immutable Audit Log

Every message is logged with the policy rule matched and the action taken, feeding your SIEM in real time.

Encryption That Just Works

S/MIME, OpenPGP, and TLS key exchange happen automatically for external recipients, with no plugins required.

Where This Gap Shows Up

Credential Phishing

Fake sharing links and device-code phishing bypass MFA and land directly in an unprotected, plaintext mailbox.

CMMC 2.0 and DFARS 252.204-7012

Self-attestation is now the only check on defense contractors after third-party CMMC assessment was suspended.

ITAR and Export Control

Technical data subject to export restrictions should never sit unprotected in a native inbox.

Dual Regulatory Exposure

A materiality judgment made for investors does not resolve a separate adequate-security obligation to a federal agency.

The Value to Your Organization

Without Kiteworks

A single phished credential exposes everything a mailbox has ever held.

- Sensitive data sits as plaintext until authentication fails
- Self-attestation is the only check on DFARS 7012 controls
- Answering "what did this account touch" takes days, if it's possible at all

With Kiteworks

Policy governs the data itself, independent of who is logged in.

- Sensitive and export-controlled content is encrypted or quarantined automatically
- Continuous, immutable audit evidence closes the self-attestation gap
- Security and compliance teams answer forensic questions in hours

Ready to Close Your DIB's CMMC Compliance Gap?

www.kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.